UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE REPUBLIC OF KAZAKHSTAN, Plaintiff, -against- DOES 1-100 INCLUSIVE, Defendants.	:	15 Civ. 1900 (ER)

MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFF'S MOTION FOR A TEMPORARY RESTRAINING ORDER AND A PRELIMINARY INJUNCTION

TABLE OF CONTENTS

Page #

Preliminary Statement 1

Statement of Facts 2

A. Defendants' Hacking of Plaintiff's Computers 2

B. The Hacked Computers Are Used to Communicate With U.S.-Based Counsel 3

C. The Defendants Have Already Begun to Post Stolen Materials On Line 4

D. Plaintiff Will Be Irreparably Harmed If Defendants Are Not Enjoined From Posting Additional Stolen Materials 5

ARGUMENT

THE COURT SHOULD ISSUE A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION AGAINST DEFENDANTS 6

A. Plaintiff is Likely to Succeed on the Merits of its CFAA Claim 7

B. Plaintiff Will Suffer Irreparable Harm if Defendants Are Not Restrained and Preliminarily Enjoined From Further Dissemination of the Stolen Materials 10

C. The Balance of Hardships Favors Plaintiff 11

D. The Public Interest Favors Protecting Plaintiff's Rights 11

E. The Requested Temporary Restraining Order Should be Issued Ex Parte to Prevent Defendants from Thwarting the Relief 12

F. Plaintiff Will Make Strong Efforts to Provide Notice of the Temporary Restraining Order and Preliminary Injunction Hearing, and to Serve the Complaint 13

Conclusion 15

Plaintiff the Republic of Kazakhstan ("Plaintiff") respectfully submits this memorandum of law in support of its motion, pursuant to Fed. R. Civ. P. 65 and 18 U.S.C. § 1030(g), for a temporary restraining order and preliminary injunction.

Preliminary Statement

This application for a temporary restraining order and preliminary injunction arises out of the illegal hacking of Plaintiff's computers and of the Gmail accounts of Plaintiff's officials by persons currently unknown, identified herein as Does 1-100 ("Defendants"), in violation of The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA").

The Defendants intentionally gained unauthorized access to Plaintiff's "protected computers," a term broadly defined in 18 U.S.C. § 1030(e)(2)(B) to include "a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." The hacked computers were used for commerce and communication with the United States, including communication with U.S.-based counsel for the Republic of Kazakhstan. They are therefore "protected computers" under the CFAA, and the Defendants' unauthorized access to those computers constitutes an actionable violation of the CFAA.

Defendants stole what is believed to be thousands of Plaintiff's emails and other documents containing sensitive, proprietary, confidential, and attorney-client privileged government documents belonging to the Republic of Kazakhstan (the "Stolen Materials"). Defendants have already improperly disseminated via the internet fourteen attorney-client privileged emails originally sent by the Republic of Kazakhstan's outside counsel (some based in New York City) to their client, that were misappropriated by the Defendants from the computers of the Republic of Kazakhstan and from Gmail accounts used from time to time by officials of the Republic of Kazakhstan to conduct official government business.

Defendants' dissemination of the Stolen Materials has already irreparably harmed Plaintiff and, if Defendants are not restrained and enjoined from further dissemination, Defendants will likely further irreparably harm Plaintiff by disclosing additional privileged attorney-client communications as well as other sensitive, proprietary, and confidential government communications.

A balancing of the parties' interests weighs strongly in favor of Plaintiff. If the requested relief is denied, Plaintiff will suffer serious and irreparable harm from Defendants' further disclosure of the Stolen Materials. Defendants, however, will not suffer any cognizable injury if they are enjoined from further dissemination of the Stolen Materials.

Finally, it is in the public interest to deter and prevent computer and cyber crime, to prevent exploitation of information illegally obtained through hacking, and to protect the integrity and safety of attorney-client communications.

Accordingly, a temporary restraining order and preliminary injunction are warranted to prevent further dissemination of the Stolen Materials.

Statement of Facts

A. Defendants' Hacking of Plaintiff's Computers

On or about January 21, 2015, the Republic of Kazakhstan learned of unauthorized public postings of certain of its privileged and confidential emails, and thereby became aware that it had been hacked. (Declaration of Marat Beketayev (the "Beketayev Decl.") at ¶ 7.)

Without authorization, Defendants unlawfully accessed: (1) the computers of the Republic of Kazakhstan and (2) Gmail accounts used from time to time by officials of the Republic of Kazakhstan to conduct official government business (collectively, the "Hacked Computers"), and misappropriated what is believed to be thousands of government emails and

other documents containing sensitive, proprietary, and highly confidential government documents, including privileged communications between the Republic of Kazakhstan and its outside attorneys in the United States and elsewhere. (*Id.* at ¶ 10.)

Gmail is an email service provided by Google Inc. ("Google"). Google is headquartered in Mountain View, California, and has offices throughout the United States and elsewhere, including New York City.

Plaintiff has launched an investigation to try to determine the identity of the hackers and their confederates, the precise scope of the intrusion, and the extent of the damages caused. That investigation is ongoing. (*Id.* at ¶ 9.)

The officials whose emails and other documents have been misappropriated include Marat Beketayev, the Executive Secretary of the Ministry of Justice of the Republic of Kazakhstan, and Andrey Kravchenko, a Deputy General Prosecutor in the General Prosecutor's Office of the Republic of Kazakhstan. (*Id.* at ¶ 9.) The Hacked Computers contain a large number of emails and other documents sent or received by these officials and other officials of the Republic of Kazakhstan. (*Id.* at ¶ 10.) Many of these emails and other documents contain sensitive, proprietary, and highly confidential communications of the Ministry of Justice and/or the General Prosecutor's Office. (*Id.* at ¶ 10.) Of those, some consist of privileged communications between the Republic of Kazakhstan and its outside attorneys in the United States (including in New York City) and elsewhere. (*Id.* at ¶ 10.)

B. <u>The Hacked Computers Are Used to Communicate With U.S.-Based Counsel</u>

The Hacked Computers are connected to the internet and are used in connection with foreign commerce and communication, including with (among others) the United States. (*Id.* at __.) The Hacked Computers are used to communicate with Plaintiff's outside U.S. counsel at Curtis, Mallet-Prevost, Colt & Mosle LLP ("Curtis"), a global law firm headquartered

at 101 Park Avenue, New York, NY 10178-0061. (*Id.* at ¶ 12.) Curtis has offices in Kazakhstan. (*Id.* at ¶ 12.) All Curtis domain (@curtis.com) electronic mail is sent and received through Curtis's servers located in Curtis's highly secure production data center in Piscataway, New Jersey. (Declaration of Anthony Baselice, dated March 13, 2015, at ¶ 2.) In particular, any Curtis domain electronic mail sent to or received by persons in Curtis's offices in Kazakhstan are sent or received through the servers in Curtis's production data center in Piscataway, New Jersey. (*Id.* at ¶ 2.)

Curtis lawyers who represent and provide legal advice and assistance to the Republic of Kazakhstan include Askar Moukhidtinov, Esq. (a member of the bar of the State of Connecticut and of the Republic of Kazakhstan), and Jacques Semmelman, Esq. (a member of the bar of the States of New York, New Jersey, and Pennsylvania, and a member of the bar of this Court). (Declaration of Jacques Semmelman (the "Semmelman Declaration"), dated March 12, 2015, at ¶ 1.) Mr. Semmelman maintains his office in Curtis's New York headquarters. (*Id.* at ¶ 1.)

C. The Defendants Have Already Begun to Post Stolen Materials On Line

Defendants have already posted some of the Stolen Materials on various websites, including https://kazaword.wordpress.com, www.respublika-kaz.info, and https://www.facebook.com. (Beketayev Decl. at ¶ 13; Ex. A.)

At least fourteen emails from among the Stolen Materials have been posted to these sites. The fourteen emails consist of privileged and confidential attorney-client communications sent by Curtis or by Gomez-Acebo & Pombo, a global law firm headquartered in Madrid, Spain, that has been performing legal services on behalf of, and has been providing legal advice to, the Republic of Kazakhstan. (*Id.* at ¶ 13.)

The fourteen emails that have been publicly disclosed by the Defendants are attorney-client privileged communications from the two law firms to their mutual client, the Republic of Kazakhstan. (*Id.* at ¶ 13.) Among the senders or "cc" recipients of these misappropriated and now-public emails are Mr. Moukhidtinov and Mr. Semmelman. (*Id.* at ¶ 13.)

D. Plaintiff Will Be Irreparably Harmed If Defendants Are Not Enjoined From Posting Additional Stolen Materials

Plaintiff has already been damaged by the illegal misappropriation, and by the public dissemination of just a small portion of the Stolen Materials. (*Id.* at ¶ 14.) Plaintiff has been forced to hire attorneys and investigators in order to try to understand the scope of the intrusion and the extent of the harm caused, and to remediate the harm. (*Id.* at ¶ 14.)

It is not feasible, however, to monetize all of the damage that has already occurred, as the misappropriation and disclosure of privileged attorney-client communications, as well as other sensitive, proprietary, and confidential communications of the Ministry of Justice and the General Prosecutor's Office of the Republic of Kazakhstan, does not lend itself to quantification. (*Id.* at ¶ 15.)

Any *further* disclosure of the Stolen Materials will inevitably result in additional irreparable harm to Plaintiff, as it is likely that further disclosures of the Stolen Materials will reveal additional sensitive, proprietary, and confidential information that belongs to the Republic of Kazakhstan, including privileged communications between the Republic of Kazakhstan and its attorneys located in the U.S. and elsewhere. (*Id.* at ¶ 16.)

In contrast, Defendants will not suffer any cognizable injury if they are enjoined from further dissemination of the Stolen Material.

Accordingly, Plaintiff respectfully requests the Court to issue a temporary restraining order and, thereafter, a preliminary injunction, restraining and enjoining the Defendants, their affiliates, employees, agents, and representatives, and all persons acting in concert with or participating with them, from using, disclosing, disseminating, posting, displaying, sharing, distributing, hosting, copying, viewing, accessing, providing access to or making available to anyone, any of the Stolen Materials, so that damage may be limited to what has already occurred and what has already been publicly disseminated by the Defendants, and so that further irreparable harm can be minimized.

ARGUMENT

THE COURT SHOULD ISSUE A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION AGAINST DEFENDANTS

Pursuant to Federal Rule of Civil Procedure 65 and 18 U.S.C. § 1030(g), the Court should issue a temporary restraining order and a preliminary injunction, to prevent further irreparable harm, and to maintain the *status quo* by directing that no additional Stolen Materials be disseminated during the pendency of the case.

To be entitled to preliminary equitable relief, a plaintiff must establish: (1) a likelihood of success on the merits; (2) that it is likely to suffer irreparable harm in the absence of preliminary relief; (3) that the balance of equities tips in its favor; and (4) that an injunction is in the public interest. *See Salinger v. Colting*, 607 F.3d 68, 77 (2d Cir. 2010).

As shown below, Plaintiff readily meets this standard. First, there is a very high likelihood that Plaintiff will succeed on the merits. Defendants' unauthorized access to the Plaintiff's protected computers violates the CFAA.

Second, Plaintiff has already been irreparably harmed through the improper dissemination of privileged attorney-client communications, and will continue to be irreparably harmed if the Defendants are not restrained and enjoined from further dissemination of the Stolen Materials.

Third, no legitimate interests of the Defendants will be harmed if a temporary restraining order and preliminary injunction are issued. The Defendants have no legitimate interest in further exploiting and disseminating the Stolen Materials.

Fourth, the public interest weighs heavily in favor of relief because the public has a strong interest in deterring and preventing computer and cyber crime, in preventing exploitation of information illegally obtained through hacking, and in maintaining the integrity and safety of attorney-client and other sensitive, proprietary, and confidential government communications.

Because consideration of each of these factors weighs heavily in Plaintiff's favor, and no factor weighs in favor of Defendants, the Court should issue a temporary restraining order and preliminary injunction enjoining Defendants, their affiliates, employees, agents, and representatives, and all persons acting in concert with or participating with Defendants, from using, disclosing, disseminating, posting, displaying, sharing, distributing, hosting, copying, viewing, accessing, providing access to or making available to anyone, in any manner whatsoever, any of the Stolen Materials.

A. Plaintiff is Likely to Succeed on the Merits of its CFAA Claim

Plaintiff is likely to succeed on the merits of its CFAA claim. The CFAA has an extremely broad sweep that prohibits knowingly accessing a "protected computer" (as defined in the CFAA) without authorization. The breadth of the CFAA's applicability is exemplified by its definition of "protected computer," which includes "a computer located outside the United States

that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B). The Hacked Computers in this case are therefore "protected computers" because, as noted above, they were used for commerce and communication with the United States, including communication with U.S.-based counsel for the Republic of Kazakhstan. (Beketayev Decl. ¶ 13)

Under the CFAA, anyone who commits any of the following acts is guilty of a crime:

- "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer" (18 U.S.C. § 1030(a)(2)(C));
- "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage" (18 U.S.C. § 1030(a)(5)(B)); or
- "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss." (18 U.S.C. § 1030(a)(5)(C)).

In addition to criminal penalties, the CFAA provides a civil cause of action for monetary and injunctive relief to a victim of a CFAA violation: "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and ***injunctive relief*** or other equitable relief." 18 U.S.C § 1030(g) (emphasis added).

Defendants intentionally accessed the Hacked Computers without authorization, and misappropriated the Stolen Materials in violation of 18 U.S.C. § 1030(a)(2)(C). *See FXDirectDealer, LLC v. Abadi*, No. 12 Civ. 1796 (CM), 2012 U.S. Dist. LEXIS 49588, at *17 (S.D.N.Y. Apr. 5, 2012) ("While the Second Circuit has yet to decide what constitutes 'access'

for the purposes of the CFAA, courts in other circuits have interpreted 'access' consistently with the word's common definition.") (internal citation and quotation omitted).

Further, Defendants' intentional and unauthorized accessing of Plaintiff's protected computers has resulted in substantial damages and loss, including the costs associated with remediating the unauthorized access, in violation of 18 U.S.C. § 1030(a)(5)(B) and (a)(5)(C). *See FXDirectDealer*, 2012 U.S. Dist. LEXIS 49588, at *17 ("An individual is liable for any damages that result from an unauthorized access, so long as he or she intentionally secured unauthorized access, regardless of whether the individual intended to cause the damages the resulted, or were recklessly indifferent as to whether they did so.") (internal citation and quotation omitted); (Beketayev Decl. at ¶ 14.) Plaintiff has invested considerable resources investigating and trying to remediate the Defendants' intrusion into these computers. (Beketayev Decl. at ¶ 14.) *See Nexans Wires S.A. v. Sark-USA, Inc.*, 166 Fed. Appx. 559, 563 (2d Cir. 2006) ("damages" and "loss" under the CFAA refer to, *inter alia*, "investigating and remedying damage to a computer").

Defendants' unauthorized access and hacking of Plaintiff's computers is precisely the type of activity the CFAA prohibits. *See, e.g., FXDirectDealer, LLC*, 2012 U.S. Dist. LEXIS 49588, at *21 (issuing injunction under the CFAA against known and unknown computer hackers prohibiting further hacking and withdrawal of funds gained as a result of the hacking activities); *JBCHoldings NY, LLC v. Pakter*, 931 F. Supp. 2d 514, 521 (S.D.N.Y. 2013) ("There is no doubt that the CFAA applies to an 'outside' hacker who remotely enters a computer system without authority to do so."); *Guest-Tek Interactive Entm't, Inc. v. Pullen*, 665 F. Supp. 2d 42, 45 (D. Mass. 2009) (the majority of CFAA cases involve hacking activities).

Accordingly, Plaintiff is likely to succeed on the merits of its CFAA claim.

B. **Plaintiff Will Suffer Irreparable Harm if Defendants Are Not Restrained and Preliminarily Enjoined From Further Dissemination of the Stolen Materials**

Plaintiff will continue to suffer irreparable harm if Defendants are not restrained and preliminarily enjoined from further dissemination of the Stolen Materials. The Second Circuit defines "irreparable harm" as "certain and imminent harm for which a monetary award does not adequately compensate." *Wisdom Imp. Sales Co., L.L.C. v. Labatt Brewing Co., Ltd.*, 339 F.3d 101, 113 (2d Cir. 2003). To prove irreparable harm, a plaintiff must demonstrate that it will suffer an injury that is neither remote nor speculative, but actual and imminent, and one that cannot be remedied if a court waits until the end of trial to resolve the harm. *Id.* (citation omitted). Here, the harm to Plaintiff – further disclosure of Stolen Materials – is virtually certain, imminent, ongoing, and not adequately compensable through money damages.

Importantly, courts have recognized that "[o]nce confidential attorney-client communications are disclosed, their confidential nature is permanently and irrevocably impaired." *X Corp. v. Doe*, 805 F. Supp. 1298, 1304 (E.D. Va. 1992) (granting preliminary injunction to prevent disclosure of potentially privileged attorney-client communication). Thus, even if Plaintiff were to ultimately prevail, its "right to prevent disclosures of confidential information might be forever lost absent an injunction." *Id.*; *see also Council on American-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 77 (D.D.C. 2009) (the disclosure of certain materials, including attorney-client privileged information, constitutes irreparable harm).

Defendants have already posted at least fourteen emails from among the Stolen Materials to various publicly available websites. (Beketayev Decl. at ¶ 13.) These fourteen emails are attorney-client privileged communications from two law firms (one based in New York City) to their mutual client, the Republic of Kazakhstan. (*Id.* at ¶ 13.) The harm from such disclosure cannot be quantified and is irreparable. (*Id.* at ¶ 15.) Any further disclosure of the

Stolen Materials will inevitably result in additional irreparable harm to Plaintiff, as it is likely that further disclosures of the Stolen Materials will reveal additional sensitive, proprietary, and confidential information that belongs to the Republic of Kazakhstan, including privileged communications between the Republic of Kazakhstan and its attorneys located in the U.S. and elsewhere. *See X Corp.*, 805 F. Supp. at 1303-04 (granting preliminary injunction to prevent disclosure of potentially privileged attorney-client communication).

C. The Balance of Hardships Favors Plaintiff

The balance of hardships tips decidedly in Plaintiff's favor. As described above, if the requested relief is denied, Plaintiff will suffer serious and irreparable harm from Defendants' further disclosure of the Stolen Materials. By contrast, Defendants will not suffer any cognizable injury at all if they are enjoined from further dissemination of the Stolen Materials. The Stolen Materials were misappropriated after Defendants illegally hacked into Plaintiff's computers and into Gmail accounts used from time to time by officials of the Republic of Kazakhstan to conduct official government business. The Defendants have no rights to the Stolen Materials. *See FXDirectDealer, LLC*, 2012 U.S. Dist. LEXIS 49588, at *19 (granting preliminary injunction based upon violations of Sections 1030(a)(4) and (5) of the CFAA, and holding that the "Defendants would suffer no cognizable harm from the injunction; their unlawful trading profits would merely be frozen, and they would be prevented from disseminating a computer program that likely has no legal purpose"). Thus, balancing the parties' respective hardships favors Plaintiff.

D. The Public Interest Favors Protecting Plaintiff's Rights

The final factor seeks confirmation that granting injunctive relief would be in the public interest. *See Salinger*, 607 F.3d at 79-80. The public has an interest in deterring and preventing computer and cyber crime, and in preventing exploitation of information illegally

obtained through hacking. In addition, the public has an interest in seeing that the integrity and safety of attorney-client communications is protected. *See X Corp.*, 805 F. Supp. at 1311 (enjoining the disclosure of attorney-client communications because, *inter alia*, "public policy strongly favors enforcing the principles of attorney confidentiality"). Thus, granting the relief requested would be in the public interest.

E. The Requested Temporary Restraining Order Should be Issued *Ex Parte* to Prevent Defendants from Thwarting the Relief

Absent a temporary restraining order granting the relief requested herein, the injury to Plaintiff will continue unabated, irreparably harming Plaintiff. For the relief to be effective at all, the temporary restraining order should be issued *ex parte*. Rule 65 of the Federal Rules of Civil Procedure permits an *ex parte* temporary restraining order where the moving party sets forth facts that show immediate and irreparable injury, and that explain why providing notice would likely lead to further irreparable harm. *See* Fed. R. Civ. P. 65(b)(1); *see Granny Goose Foods, Inc. v. Teamsters*, 415 U.S. 423, 438-39 (1974) ("*Ex parte* temporary restraining orders are no doubt necessary in certain circumstances . . . .").

To date, some fourteen emails (out of the potentially thousands in the Stolen Materials) have been posted on the internet. (Beketayev Decl. ¶ 13.) If notice is given to Defendants prior to the issuance of a temporary restraining order, Defendants will be motivated to quickly post much more – if not all – of the remaining Stolen Materials on public internet pages in an effort to thwart any provisional relief issued by the Court. (Semmelman Decl. at ¶ 10.) By that point, all the sensitive, proprietary, confidential, and attorney-client privileged government documents stolen from Plaintiff will have been made publicly available by Defendants, which will render null the provisional relief requested herein. The irreparable harm to Plaintiff will be immense, as Plaintiff's sensitive, proprietary, confidential, and attorney-client

privileged government documents will be available to anyone with an internet connection. (*Id.* at ¶ 11.) Under these circumstances, the Court should grant the temporary restraining order on an *ex parte* basis. *See In re Vuitton Et Fils S.A.*, 606 F.2d 1, 4 (2d Cir. 1979) (per curiam) (notice prior to issuing temporary restraining order was not warranted where notice would "serve only to render fruitless further prosecution of the action").

F. Plaintiff Will Make Strong Efforts to Provide Notice of the Temporary Restraining Order and Preliminary Injunction Hearing, and to Serve the Complaint

To ensure due process, immediately upon entry of the requested *ex parte* temporary restraining order, Plaintiff will undertake strong efforts to provide notice of the preliminary injunction hearing to Defendants, and to serve the Complaint.

The Defendants are as yet unidentified. (Semmelman Decl. at ¶ 13.) As such, neither Plaintiff nor its counsel has any personal contact information for them. (*Id.* at ¶ 13.) However, Plaintiff and its counsel have access to the two Facebook pages on which some of the Stolen Materials were posted. (*Id.* at ¶ 15.) Facebook has a functionality through which a logged-in user may post a "comment" to a post. (*Id.* at ¶ 14.) This comment is public, and may be seen by any internet user who views the page. (*Id.* at ¶ 15.) The two Facebook pages at issue have this functionality. (*Id.* at ¶ 15.)

Because neither Plaintiff nor its counsel currently has any alternative method for directly contacting the Defendants, counsel will provide notice to the Defendants after the temporary restraining order is issued by posting a "comment" in substantially the following form on the two Facebook pages:

> On March 12, 2015, a Complaint was filed against you by the Republic of Kazakhstan in the United States District Court for the Southern District of New York. The case is styled as *The Republic of Kazakhstan v. Does 1-100 Inclusive*, 15 Civ. 1900 (ER)

(S.D.N.Y. 2015). A copy of the Complaint can be found at the following link: _____.

In addition, a Motion for a Temporary Restraining Order and Preliminary Injunction (the "Motion") has been filed against you. A copy of the Motion and supporting papers can be found at the following link: _____. The Motion is brought by Order to Show Cause so that the matter will proceed on an expedited basis.

An *ex parte* temporary restraining order has already been issued against you, enjoining you, your affiliates, employees, agents, and representatives, and all persons acting in concert with or participating with you, from using, disclosing, disseminating, posting, displaying, sharing, distributing, hosting, copying, viewing, accessing, providing access to or making available to anyone, in any manner whatsoever, the materials stolen by you from the computer system of the Republic of Kazakhstan and from the Gmail accounts of officials of the Republic of Kazakhstan.

A copy of the Order to Show Cause can be found at the following link: _____. The Court has directed the parties to appear before it with respect to the Preliminary Injunction on _____ at the following location: the United States Courthouse for the Southern District of New York, 40 Foley Square, New York, NY 10007.

If you are represented by an attorney, please let us know and we will notify your counsel of the date and time selected by the Court.

Curtis, Mallet-Prevost, Colt & Mosle LLP

101 Park Avenue

New York, NY 10178-0061

Att: Jacques Semmelman, Esq.

jsemmelman@curtis.com

Attorneys for the Republic of Kazakhstan

(*Id.* at ¶ 16.)

Because the Defendants are anonymous, the most practical way of providing them with actual notice of these proceedings is by posting the notice on the very Facebook pages that contain the postings of the fourteen emails drawn from the Stolen Materials. It is reasonable to

expect that the Defendants will monitor these pages and that they will therefore see the notice of these proceedings.

The two Facebook pages at issue were created in February of 2015. (Semmelman Decl. at ¶ 15.) Since then, other users have posted comments on the pages. (*Id.* at ¶ 15.)

In addition, Plaintiff will post a notice of these proceedings in two newspapers of general circulation in the Republic of Kazakhstan, namely Kazakhstanskaya Pravda (published in Russian) and Egemen Kazakhstan (published in Kazakh), once a day for thirty days. *See S.E.C. v. Tome*, 833 F.2d 1086, 1093-94 (2d Cir. 1987) (holding that notice published every day for four weeks in the *International Herald Tribune* was sufficient).

The Court can authorize these methods of service under Federal Rule of Civil Procedure 4(f)(3) which authorizes service by "other means" that are "not prohibited by international agreement." *Gurung v. Malhotra*, 279 F.R.D. 215, 218 (S.D.N.Y. 2011). A party need not have attempted every permissible means of service before petitioning the court for alternative relief under Rule 4(f)(3), as it stands on equal footing with other methods of service authorized by Rule 4. *See Ryan v. Brunswick Corp.*, No. 02-CV-0133E(F), 2002 U.S. Dist. LEXIS 13837, at *2 (W.D.N.Y. May 31, 2002) (Rule 4(f)(3) "is neither 'extraordinary relief' nor a 'last resort' to be used only when parties are unable to effectuate service under (f)(l) or (f)(2)").

Notice and service by the foregoing means satisfy due process, are appropriate, sufficient, and reasonable to apprise Defendants of this action, and are necessary under the circumstances. Plaintiffs therefore request that the Court approve and order the alternative means of service discussed above.

Conclusion

Plaintiff has satisfied each element of the standard for issuance of a temporary restraining order and a preliminary injunction. Accordingly. Plaintiff respectfully requests that

the Court issue a temporary restraining order enjoining Defendants, their affiliates, employees, agents, and representatives, and all persons acting in concert with or participating with Defendants, from using, disclosing, disseminating, posting, displaying, sharing, distributing, hosting, copying, viewing, accessing, providing access to or making available to anyone, in any manner whatsoever, any of the Stolen Materials.

Plaintiff further requests that the Court issue a preliminary injunction:

a) Enjoining Defendants, their affiliates, employees, agents, and representatives, and all persons acting in concert with or participating with Defendants, from using, disclosing, disseminating, posting, displaying, sharing, distributing, hosting, copying, viewing, accessing, providing access to or making available to anyone, in any manner whatsoever, any of the materials stolen by the Defendants from the computer system of Plaintiff and Gmail accounts of the Plaintiff's officials (the "Stolen Materials");

b) Ordering that Defendants, their affiliates, employees, agents, and representatives, and all persons acting in concert with or participating with Defendants immediately deliver to Plaintiff: (i) all copies of the Stolen Materials; and (ii) all copies of any materials (in paper, electronic, or any other form) that contain or reflect any information derived from the Stolen Materials; and

c) Ordering that Defendants, their affiliates, employees, agents, and representatives, and all persons acting in concert with or participating with Defendants, turn over to the Court any proceeds that Defendants have

received as a result of their misappropriation and use of the Stolen Materials, such proceeds to be held in constructive trust until the conclusion of this litigation.

Dated: New York, New York
March, 13, 2015

Respectfully submitted,

CURTIS, MALLET-PREVOST,
COLT & MOSLE LLP

By: _____

Jacques Semmelman (JS 5020)
jsemmelman@curtis.com
Michael R. Graif (MG 4795)
mgraif@curtis.com

101 Park Avenue
New York, New York 10178
(212) 696-6000

Attorneys for Plaintiff the Republic of Kazakhstan